Amendments to the Claims:

This listing of claims will replace all prior version, and listings, of claims in the application.

Listing of Claims:

1 (Currently amended) A method for protecting software from unauthorized use on a computer system using an external security device, the method comprising the steps of:

(a) encrypting the software to be protected using an encryption key, creating encrypted software, wherein the encryption key is derived from a dynamic key, which is assigned to the software to be protected and does not change between copies of the software;

(b) in response to the security device being coupled to the computer system, sending information identifying the protected software from the computer system to the security device;

~~(b)~~(c) ~~authorizing use of the software on the computer system by generating the encryption key within the security device~~ using information supplied from the software to determine if the dynamic key assigned to the software is present in the security device, and if so, generating the encryption key within the security device using the dynamic key; and

~~(c)~~(d) authorizing use of the software on the computer system by sending the encryption key from the security device to the computer system for decryption of the software.

2 (Currently Amended) The method of claim 1 wherein step (a) further includes the steps of:

(i) generating the encryption key using at least ~~first and second pieces of information to generate an encryption key~~ the dynamic key and a first piece of information;

(ii) ~~associating~~ providing the first piece of information with the encrypted software; and

(iii) storing the ~~second piece of information~~dynamic key in the security device.

3 (Currently Amended) The method of claim 2 wherein step (b) further includes the steps of:

(i) sending the first piece of information ~~associated~~ provided with the encrypted software to the security device, and

(ii) using the first piece of information and the ~~second piece of information~~dynamic key to generate the encryption key in the security device.

4 (Currently Amended) The method of claim 2 further including the steps of:

generating a second encryption key using the dynamic key and the first ~~and second piecespiece~~ of information;

providing the second encryption key with the encrypted software;

during software authorization, generating the second encryption key on the security device using the dynamic key and the first ~~and second piecespiece~~ of information;

using the second encryption key to encrypt the first encryption key generated on security device prior to transmitting the first encryption key to the computer system; and

when the encrypted first encryption key is received on the computer system, using the second encryption key provided with the encrypted software to decrypt the first encryption key.

5 (Previously Amended) The method of claim 2 further including the steps of:

generating a random number on the computer system;

transmitting the random number to the security device along with the first piece of information;

scrambling the encryption key generated by the security device by performing a reversible mathematical operation on the encryption key using the random number;

encrypting the scrambled encryption key and transmitting the encrypted scrambled encryption key to the computer system; and

performing a reverse of the reversible mathematical operation performed within the security device using the random number to descramble the encryption key after the encrypted scrambled encryption key is decrypted on the computer system.

6 (Currently Amended) The method of claim 2 further including the step of: using an initialization vector ~~and a dynamic key~~ as the first ~~and second pieces~~ piece of information.

7 (Original) The method of claim 6 further including step of: using a security key as the encryption key and a communications key as the second encryption key.

8 (Original) The method of claim 7 further including the step of: embedding a mathematical algorithm within the security device to create the communications key and the security key from the dynamic key and the initialization vector.

9 (Original) The method of claim 8 further including the step of: including the encrypted software with an authentication program, wherein the authentication program is embedded within a separate security processor provided in conjunction with the co-processors.

10 (Original) The method of claim 9 further including the step of: sharing memory between the security processor and the co-processors and decrypting the encrypted software in the shared memory.

11 (Original) The method of claim 10 further including the step of: preventing the software from running in any of the co-processors unless the software has first been decrypted by the security processor.

12 (Original) The method of claim 6 wherein the initialization vector is created from a checksum of encrypted software to be protected.

13 (Original) The method of claim 6 further including the step of: associating a product ID with the software and transferring the product ID to the security device along with the initialization vector.

14 (Original) The method of claim 13 further includes the step of: providing multiple storage locations within the security device to enable storing multiple dynamic keys and corresponding product IDs.

15 (Original) The method of claim 14 further includes the step of: using the product ID code to locate and select the appropriate dynamic key within the security device when receiving an authorization request.

16 (Currently Amended) A method for protecting software from unauthorized use on a computer system, the method comprising the steps of:

(a) using at least a dynamic key and a first ~~and second piecespiece~~ of information to generate an encryption key, wherein the dynamic key is assigned to the software to be protected and does not change between copies of the software;

(b) encrypting the software using the encryption key;

(c) ~~associating~~ providing the first piece of information with the encrypted software, wherein at least a portion of the first piece of information identifies the protected software;

(d) storing the ~~second piece of information~~dynamic key in a security device; and

(e) authorizing use of the software after the encrypted software is loaded on the computer system and the security device is coupled to the computer system by,

(i) sending the first piece of information ~~associated~~ provided with the encrypted software to the security device,

(ii) if the dynamic key assigned to the software is present in the security device, using the first piece of information and the ~~second piece of information~~dynamic key to generate the encryption key in the security device,

(iii) transmitting the encryption key from the security device to the computer system, and

(iv) decrypting the encrypted software with the encryption key for use on the computer system.

17 (Previously Amended) The method of claim 16 further including the step of:

(v) discarding the encryption key after decryption of the encrypted software.

18 (Currently Amended) The method of claim 17 further including the steps of:

generating a second encryption key using the dynamic key and the first ~~and second piecespiece~~ of information;

providing the second encryption key with the encrypted software;

during software authorization, generating the second encryption key on the security device using the dynamic key and the first ~~and second piecespiece~~ of information;

~~a~~using the second encryption key to encrypt the first encryption key generated on security device prior to transmitting the first encryption key to the computer system; and

when the encrypted first encryption key is received on the computer system, using the second encryption key provided with the encrypted software to decrypt the first encryption key.

19 (Previously Amended) The method of claim 16 further including the steps of:

generating a random number on the computer system;

transmitting the random number to the security device along with the first piece of information;

scrambling the encryption key generated by the security device by performing a reversible

mathematical operation on the encryption key using the random number;

encrypting the scrambled encryption key and transmitting the encrypted scrambled encryption key to the computer system; and

performing a reverse of the reversible mathematical operation performed within the security device using the random number to descramble the encryption key after the encrypted scrambled encryption key is decrypted on the computer system.

20 (Currently Amended) The method of claim 16 further including the step of: using an initialization vector and a ~~key as product ID code as~~ the first ~~and second piecespiece~~ of information.

21 (Original) The method of claim 20 further including steps of: using a security key as the encryption key and a communications key as the second encryption key.

22 (Currently Amended)A method for protecting software from unauthorized use on a computer system, the method comprising the steps of:

(a) creating an initialization vector and a dynamic key, wherein the is assigned to the software to be protected and does not change between copies of the software;

(b) using the initialization vector and the dynamic key to generate a security key;

(c) using the security key and the initialization vector to generate a communication key;

(d) encrypting software using the security key to create encrypted software;

(e) creating a software package comprising the initialization vector, the encrypted software, the communications key, and an authentication program;

(f) storing the dynamic key in a security device;

(g) authorizing use of the software after the software package has been loaded on the computer system and the security device coupled to the computer system by

(i) sending the initialization vector to the security device,

(ii) in the security device, using the initialization vector and the ~~store~~ stored dynamic key to generate the security key and communication key if the dynamic key assigned to the software is present in the security device,

(iii) encrypting the security key using the communication key,

(iv) sending the encrypted security key to the computer system as a response,

(v) using the communications key in the software package to decrypt encrypted security key, and

(vi) using the security key to decrypt the encrypted software for use on the computer system.

23 (Original) The method of claim 22 further including the steps of:

generating a random number on the computer system;

transmitting the random number to the security device;

scrambling the security key generated by the security device by performing a reversible mathematical operation on the security key using the random number;

encrypting the scrambled encryption key and transmitting the encrypted scrambled security key to the computer system; and

performing a reverse of the reversible mathematical operation performed within the security device using the random number to descramble the security key after the encrypted scrambled security key is decrypted on the computer system.

24 (Currently amended) A computer-readable medium containing program instructions for protecting software from unauthorized use on a computer system using an external security device, the program instructions for:

(a) encrypting the software to be protected using an encryption key, creating encrypted software, wherein the encryption key is derived from a dynamic key, which is assigned to the software to be protected and does not change between copies of the software;

(b) in response to the security device being coupled to the computer system, sending information identifying the protected software from the computer system to the security device;

~~(b)~~(c) authorizing use of the software on the computer system by generating the ~~encryption key within the security device~~ using information supplied from the software to determine if the dynamic key assigned to the software is present in the security device, and if so, generating the encryption key within the security device using the dynamic key; and

~~(c)~~(d) authorizing use of the software on the computer system by sending the encryption key from the security device to the computer system for decryption of the software.

25 (Currently Amended) The computer-readable medium of claim 24 wherein instruction (a) further includes the instructions for:

(i) generating the encryption key using at least ~~first and second pieces of information to generate an encryption key~~ the dynamic key and a first piece of information;

(ii) ~~associating~~ providing the first piece of information with the encrypted software; and

(iii) storing the ~~second piece of information~~ dynamic key in the security device.

26 (Currently Amended) The computer-readable medium of claim 25 wherein instruction (b) further includes the instructions for:

(i) sending the first piece of information ~~associated~~ provided with the encrypted software to the security device, and

(ii) using the first piece of information and the ~~second piece of information~~dynamic key to generate the encryption key in the security device.

27 (Currently Amended) The computer-readable medium of claim ~~26~~ 25 further including the instructions for:

generating a second encryption key using the dynamic key and the first ~~and second piecespiece~~ of information;

providing the second encryption key with the encrypted software;

during software authorization, generating a second encryption key on the security device using the dynamic key and the first ~~and second piecespiece~~ of information;

a using the second encryption key to encrypt the first encryption key generated on security device prior to transmitting the first encryption key to the computer system; and

when the encrypted first encryption key is received on the computer system, using the second encryption key provided with the encrypted software to decrypt the first encryption key.

28 (Currently Amended) The computer-readable medium of claim ~~24~~ 25 further including the instructions for:

generating a random number on the computer system;

transmitting the random number to the security device along with the first piece of information;

scrambling the security key generated by the security device by performing a reversible mathematical operation on the encryption key using the random number;

encrypting the scrambled encryption key and transmitting the encrypted scrambled encryption key to the computer system; and

performing a reverse of the reversible mathematical operation performed within the security device using the random number to descramble the encryption key after the encrypted scrambled encryption key is decrypted on the computer system.

29 (Currently Amended) The computer-readable medium of claim 25 further including the instruction for: using an initialization vector ~~and a dynamic key~~ as the first ~~and second piecespiece~~ of information.

30 (Original) The computer-readable medium of claim 29 further including instruction for: using a security key as the encryption key and a communications key as the second encryption key.

31 (Original) The computer-readable medium of claim 30 further including the instruction for: embedding a mathematical algorithm within the security device to create the communications key and the security key from the dynamic key and the initialization vector.

32 (Original) The computer-readable medium of claim 31 further including the instruction for: including the encrypted software with an authentication program, wherein the authentication program is embedded within a separate security processor provided in conjunction with the co-processors.

33 (Original) The computer-readable medium of claim 32 further including the instruction for: sharing memory between the security processor and the co-processors and decrypting the encrypted software in the shared memory.

34 (Original) The computer-readable medium of claim 33 further including the instruction for: preventing the software from running in any of the co-processors unless the software has first been decrypted by the security processor.

35 (Original) The computer-readable medium of claim 25 wherein the initialization vector is created from a checksum of encrypted software to be protected.

36 (Original) The computer-readable medium of claim 29 further including the instruction for: associating a product ID with the software and transferring the product ID to the security device along with the initialization vector.

37 (Original) The computer-readable medium of claim 36 further includes the instruction for: providing multiple storage locations within the security device to enable storing multiple dynamic keys and corresponding product IDs.

38 (Original) The computer-readable medium of claim 37 further includes the instruction for: using the product ID code to locate and select the appropriate dynamic key within the security device when receiving an authorization request.

39 (Original) A computer software authentication system comprising:

a computer system;

a software package loaded on the computer system that includes,

an encrypted software program encrypted with a first encryption key,

an authorization program,

a first key of a keyset, and

a second encryption key; and

a security device in communication with the computer system that includes a second key of the keyset and mathematical algorithms,

wherein when the software package is executed the computer system, the encrypted software program is authenticated by,

transferring the first key of the keyset from the authorization program to the security device,

generating in the security device the first and second encryption keys using the keyset and the mathematical algorithms,

encrypting the first encryption key using the second encryption key,

transferring the encrypted first encryption key from the security device to the computer system,

decrypting the encrypted first encryption key on the computer system using the second encryption key included in the software package, and

using the first encryption key to decrypt the encrypted software for execution on the computer system.

40 (New) A method for protecting software from unauthorized use on a computer system as using an external security device, the method comprising the steps of:

(a) encrypting the software to be protected using an encryption key that is mathematically derived from an dynamic key;

(b) imbedding in the protected software a communications key that is also derived from an dynamic key ;

(c) authorizing the use of the software, only if the dynamic key is present in the security device, by generating the encryption key from the dynamic key within the security device;

(d) encrypting the encryption key with the communications key within the security device and sending the encrypted encryption key from the security device to the computer system; and

(e) with the communications key imbedded in the software, decrypting the encryption key and using the encryption key to decrypt the software.

41 (New) The method of claim 40 wherein step (c) further includes the step of: providing information from the software to the security device and using the information during generation of the encryption key, such that different encryption keys can be derived by having the software provide different information.

42 (New) The method of claim 41 wherein step (c) further includes the step of: transmitting a random number from the software to the external security device for use during encryption of the encryption key so that this result appears random.